

Z

A R E S

S E C U R I T Y

Protecting the World's Most Critical Assets

You've Been Compromised



Locky Ransomware Message

!!! IMPORTANT INFORMATION !!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.

More information about the RSA and AES can be found here:

[links to Wikipedia]

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.

To receive your private key follow one of the links:

[links to .onion sites accessible via Tor browser]

If all of this addresses are not available, follow these steps:

[Instructions how to install Tor browser]

!!! Your personal identification ID: [ID number] !!!



Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

CMT from Monday to Friday

Payment will be raised on

5/15/2017 15:47:30

Time Left

02:22:56:35

Your files will be lost on

5/19/2017 15:47:30

Time Left

06:22:56:35

[About bitcoin](#)

[How to buy bitcoins?](#)



Send \$300 worth of bitcoin to this address:

115p7UMMngoj1pMvvpHijcRdfJNXj6LrLn

Copy

- ▶ **Your limited resources are fighting unlimited resources**
- ▶ **Assume you will be hacked!**
- ▶ **The question is, how will you minimize the impact?**
 - ▶ **a near miss**
 - ▶ **a flesh wound**
 - ▶ **or a lethal blow**
- ▶ **Have you implemented the elements of a cyber incident recovery (NIST Special Publication 800-184)?**
- ▶ **Will you report on the incident to improve preparation for a similar incident in the future?**

REAL WORLD INCIDENT RESPONSE


Computer is left on over night

Employee arrives at work to find :

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English



Payment will be raised on

5/15/2017 15:47:30

Time Left

02:22:56:36

Your files will be lost on

5/19/2017 15:47:30

Time Left

06:22:56:36

What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?


Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

[About bitcoin](#)

[How to buy bitcoins?](#)

 **bitcoin**
ACCEPTED HERE

Send \$300 worth of bitcoin to this address:

115p7UMMngo1pMvKpHijcRdfJNXj6LrLn

Copy

- ▶ **Identification**
 - ▶ **Employee calls the Help Desk**
 - ▶ **Help Desk recognizes the message (if applicable engage Computer Incident Response Team plan) and works to**
- ▶ **Contain the virus:**
 - ▶ **Disconnects the impacted computer from network**
 - ▶ **Has the employee shut down the computer to prevent further corruption**
 - ▶ **Identifies backup data to verify it was not corrupted**
- ▶ **Eradication of the threat:**
 - ▶ **Computer is restarted in safe mode**
 - ▶ **Restoration to a previous date**
 - ▶ **Operating System updates applied**
 - ▶ **Virus scan completed to remove corrupted files**

INCIDENT RESPONSE

- ▶ **Recovery**
 - ▶ Files from backup are loaded
 - ▶ User is given refresher training on suspect emails and attachments
 - ▶ User changes passwords
 - ▶ IT department verifies all computational resources are scanned and have current updates
 - ▶ Firewall parameters are audited and updated to further protect for potential malicious activity
- ▶ **Lessons Learned**
 - ▶ IT modifies individual PC upgrade procedures to include auditing all computer assets on a scheduled basis
 - ▶ Firewall updates and modifications are scheduled for standard intervals and to be updated when new threats were identified
 - ▶ Organizational security tips are added to weekly distributions

INCIDENT RESPONSE – CONTD.

- ▶ Overall process similar for most incidents
 - ▶ With minor incident-specific variations
- ▶ Described in NIST 800-61 rev.2
 - ▶ Preparation
 - ▶ Detection and Analysis
 - ▶ Containment, Eradication, and Recovery, and
 - ▶ Post-Incident Analysis



- ▶ **First step in creating an incident response plan**
- ▶ **Not an enumeration process**
 - ▶ Listing all possible threat scenarios
 - ▶ And appropriate response to each of these scenarios
- ▶ **More productive**
 - ▶ Identify basic steps common to all events
 - ▶ Plan execution of each of these steps

PREPARATION

A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, set against the blue background.

- ▶ **Peacetime activity**
 - ▶ **Incident response policy**
 - ▶ **Incident response team**
 - ▶ **Supporting team**
 - ▶ **Incident communication**
 - ▶ **Regulatory Compliance**
 - ▶ **Hardware and software updates**
 - ▶ **Training**

**INCIDENT PREPARATION
COMPONENTS**

A decorative graphic consisting of several parallel white lines of varying lengths and orientations, located in the bottom right corner of the slide.

- ▶ **Description of standard methods used by organization for handling information Security Incidents**
- ▶ **Benefits of policy**
 - ▶ **Helps focus on incident as a whole, from start to finish**
 - ▶ **Without getting diverted by media and organizational pressures**
 - ▶ **Discussions provide management with understanding of issues they may have to deal with during an actual incident**
 - ▶ **Impacts of planned controls can be assessed by stakeholders**
 - ▶ **May not be anticipated by IT team**
 - ▶ **Reassurance for users**

INCIDENT RESPONSE POLICY

- ▶ **Staff designated to respond to incidents**
 - ▶ **Develop experience over time about expectations of organization during incidents**
 - ▶ **Often cross-departmental**
 - ▶ **Managers have to spare IRT members when needed**
- ▶ **Responsibilities**
 - ▶ **Quickly identifying threats to the campus data infrastructure**
 - ▶ **Assessing the level of risk**
 - ▶ **Taking immediate steps to mitigate risks**
 - ▶ **Notifying management of the event and associated risk**
 - ▶ **Notifying local personnel of any incident involving their resources**
 - ▶ **Issuing a final report as needed, including lessons learned**
- ▶ **Roles of each member of the IRT must be part of the incident response policy**
- ▶ **A large organization may need multiple IRTs**
 - ▶ **One within each division of the organization**
 - ▶ **A central group decided when events start crossing boundaries of the affected division**

INCIDENT RESPONSE TEAM

- ▶ **The IRT will have one chair, usually a senior security analyst**
 - ▶ **Coordinates with external stakeholders**
 - ▶ **Helps other IRT members to perform their functions**
 - ▶ **Needs high credibility within the organization**
 - ▶ **For competence**
 - ▶ **Excellent communication skills, both oral and in writing**
 - ▶ **Enough technical background to understand the situation**
 - ▶ **Judgment to make split second, educated decisions based on the status updates**
- ▶ **Technical members of IRT selected depending on the threat action, e.g.**
 - ▶ **If an Oracle database was breached due to a compromised administrator account on the Operating System, the IRT may include the following members**
 - ▶ **A person familiar with the OS to look at the OS system and logs**
 - ▶ **A Database Administrator to examine Oracle database, contents, and logs**
 - ▶ **Try to determine if anything was altered.**
 - ▶ **A Network Engineer to review firewall and/or netflow logs observe any unusual traffic**
 - ▶ **Desktop Services personnel if desktop machines facilitated the attack**

INCIDENT RESPONSE TEAM COMPOSITION



IRT INTERACTIONS WITH STAKEHOLDERS

- ▶ **Communication is an important aspect of the duties of the IRT**
 - ▶ **Extreme interest among different constituencies for information**
 - ▶ **Potentially conflicting needs**
 - ▶ **Often not enough information for satisfactory response**

- ▶ **Resist temptation of conveying speculation as informed “expert” opinion**

- ▶ **Need-to-know principle**
 - ▶ **People only provided information necessary to perform their job**

- ▶ **In communication with general public, supporting team advisable**
 - ▶ **Media Relations has the know-how and experience on dealing with media**
 - ▶ **Legal Counsel can verify federal or state disclosure laws**
 - ▶ **Unintended disclosure may have severe financial and public relation consequences**
 - ▶ **Law Enforcement for government cover and credibility**

- ▶ **Minimize rumor-mongering, ill-informed publicity and general disorder**

SUPPORTING TEAM

- ▶ **Inbound communications**
 - ▶ Information about occurrence of incident
- ▶ **Outbound communications**
 - ▶ Notifications to affected people



INCIDENT COMMUNICATIONS

- ▶ **Direct Report**
 - ▶ Asset owner or custodian may report the incident
 - ▶ E.g. observing unusual computer behavior
- ▶ **Anonymous Report**
 - ▶ Web forms to report an issue anonymously without fear of reprisal
 - ▶ E.g. Allegations that a high ranking University official is printing pornographic material on University printers
 - ▶ Public relations risk, sexual harassment lawsuits
- ▶ **Help Desk**
 - ▶ Problem resolution may reveal problems
 - ▶ E.g. misconfiguration of shared network drives
- ▶ **Self-Audit**
 - ▶ Periodical vulnerability assessment and log analysis may identify breaches
 - ▶ E.g. a forgotten FTP process
 - ▶ Being used as a mp3 file server

INBOUND COMMUNICATIONS

- ▶ **Affected people are curious**
- ▶ **IT Personnel and the IT Help Desk**
 - ▶ **Users quickly overwhelm Help Desk when essential assets are affected**
 - ▶ **Immediate updates to remove exploited vulnerability**
- ▶ **Inform managers and other executives periodically**
 - ▶ **Even if nothing has changed**
 - ▶ **Prevents distracting phone calls to engineers working on containment and eradication of the problem**
 - ▶ **Quick text messages and brief email messages with status updates are adequate**
- ▶ **End Users and Customers**
 - ▶ **Get very edgy when they don't know what is going on**
 - ▶ **2 questions**
 - ▶ **When will the system be back**
 - ▶ **What happened**

OUTBOUND COMMUNICATIONS

- ▶ **Act of following applicable laws, regulations, rules, industry codes and contractual obligations**
 - ▶ Ideally, best-practices developed to avoid well-known past mistakes
 - ▶ In practice, often important mainly because non-compliance leads to avoidable penalties
- ▶ **Need to comply with incident response requirements applicable to your context**
- ▶ **Example**
 - ▶ **Federal Information Security Management Act (FISMA)**
 - ▶ Requires Federal agencies to establish incident response capabilities
 - ▶ Each Federal civilian agency must designate a primary and secondary point of contact with US-CERT
 - ▶ United States Computer Emergency Readiness Team
 - ▶ Report all incidents consistent with the agency's incident response policy
 - ▶ **When known or suspected loss, theft or compromise of PII (personally identifiable information) involving US Navy systems occurs, the Department of the Navy is required to**
 - ▶ Use OPNAV Form 5211/13 to make initial and follow up reports
 - ▶ Send form US-CERT within 1 hour of discovering a breach has occurred
 - ▶ Report to the DON CIO Privacy Office within 1 hour
 - ▶ Report to the Defense Privacy Office
 - ▶ Report to Navy, USMC, BUMED chain of command, as applicable

COMPLIANCE

- ▶ **To be effective, IRT needs appropriate tools**
- ▶ **Sampling of the hardware and software recommended by NIST 800-61 rev.2 for incident response includes**
 - ▶ Backup devices to create disk images or other incident data
 - ▶ Laptops for gathering, analyzing data, and writing reports
 - ▶ Spare computer hardware for “crash and burn” purposes, such as trying out malware and other payload found and considered “unknown.”
 - ▶ Packet analyzers to capture and analyze network traffic
 - ▶ Digital forensics software to recover erased data, analyze Modified, Access, and Creation (MAC) timelines, log analysis, etc. (e.g. Figure 3)
 - ▶ Evidence gathering accessories such as digital cameras, audio recorders, chain of custody forms etc
- ▶ **Search engines are very useful**
 - ▶ Log snippet or FTP banner may reveal valuable information
 - ▶ Location of log files, configuration files, and other important clues
 - ▶ Helps the security team to build a more complete timeline for the event

HARDWARE AND SOFTWARE

- ▶ **Awareness of a baseline set of information on all aspects of security, e.g.**
 - ▶ **Access Control**
 - ▶ **Telecommunications and Network Security**
 - ▶ **Information Security Governance and Risk Management**
 - ▶ **Software Development Cryptography**
 - ▶ **Security Architecture and Design**
 - ▶ **Security Operations**
 - ▶ **Business Continuity and Disaster Recovery Planning**
 - ▶ **Legal, Regulations, Investigations and Compliance**
 - ▶ **Physical (Environmental) Security**
- ▶ **Other facets of training**
 - ▶ **Media Relations**

TRAINING

- ▶ **Documentation**
 - ▶ Record for organizational memory
 - ▶ Facilitate post-incident analysis to improve response process
- ▶ **Detection methods**
 - ▶ Use prior preparation to detect ongoing incidents
- ▶ **Analysis**
 - ▶ Identify damage
- ▶ **Overview in this chapter**
 - ▶ Details in next chapter

DETECTION AND ANALYSIS

- ▶ **NIST recommendations for minimal information**
 - ▶ **Current status of the incident**
 - ▶ **New, in progress, forwarded for investigation, resolved, etc.**
 - ▶ **Summary of the incident**
 - ▶ **Indicators related to the incident**
 - ▶ **Other incidents related to this incident**
 - ▶ **Actions taken by all incident handlers on this incident**
 - ▶ **Chain of custody, if applicable**
 - ▶ **Impact assessments related to the incident**
 - ▶ **Contact information for other involved parties**
 - ▶ **e.g., system owners, system administrators**
 - ▶ **List of evidence gathered during the incident investigation**
 - ▶ **Comments from incident handlers**
 - ▶ **Next steps to be taken**
 - ▶ **e.g., rebuild the host, upgrade an application**

INCIDENT DOCUMENTATION

1. **Visible changes to services**
 - ▶ E.g. web site defacement
2. **Performance monitoring**
 - ▶ E.g. excessively slow computer performance
3. **PII monitoring**
 - ▶ E.g. Google alerts
 - ▶ www.google.com/alerts
4. **File integrity monitoring**
 - ▶ Host based IDS tools
 - ▶ E.g. OSSEC

DETECTION METHODS



5. Anonymous report

6. Log analysis

- ▶ E.g. /var/log/messages

7. End point protection alerts

- ▶ E.g. malware protection, host IDS functionality

8. Internal investigations

- ▶ E.g. Internal audit

DETECTION METHODS



- ▶ **Begins with incident detection**
 - ▶ **Discover all adverse events that compose the incident**
 - ▶ **Manage the next phase of the cycle**
 - ▶ **Containment and Eradication**
 - ▶ **Want to avoid containment without analysis**
- ▶ **Internet Search Engines are very helpful during analysis**
 - ▶ **FTP banners, port numbers on botnets can be searched**
 - ▶ **Perspective of other experts who have faced this situation before**
- ▶ **Identify stakeholders**
- ▶ **Identify restricted or essential assets affected by incident**
 - ▶ **Primary targets for protection and eradication**

ANALYSIS

- ▶ **Containment**
 - ▶ The act of preventing the expansion of harm
 - ▶ Typically involves disconnecting affected computers from the network
 - ▶ May involve temporary shutdown of services
 - ▶ Hence needs careful thought
- ▶ **Sometimes containment is necessary before analysis is completed**
 - ▶ If the analyst is confident that ongoing events merit action
 - ▶ And/or determines that risk to assets is too high for events to continue
 - ▶ Largely determined by the experience of IRT members
 - ▶ Along with input from management, if possible
 - ▶ E.g.
 - ▶ A backdoor is being used to actively transfer PII to off-campus hosts
 - ▶ Network connection should be broken as soon as possible
 - ▶ Thereafter, the backdoor can be handled
 - ▶ E.g. through network ACLs, firewalls, or actual removal of the backdoor from the server

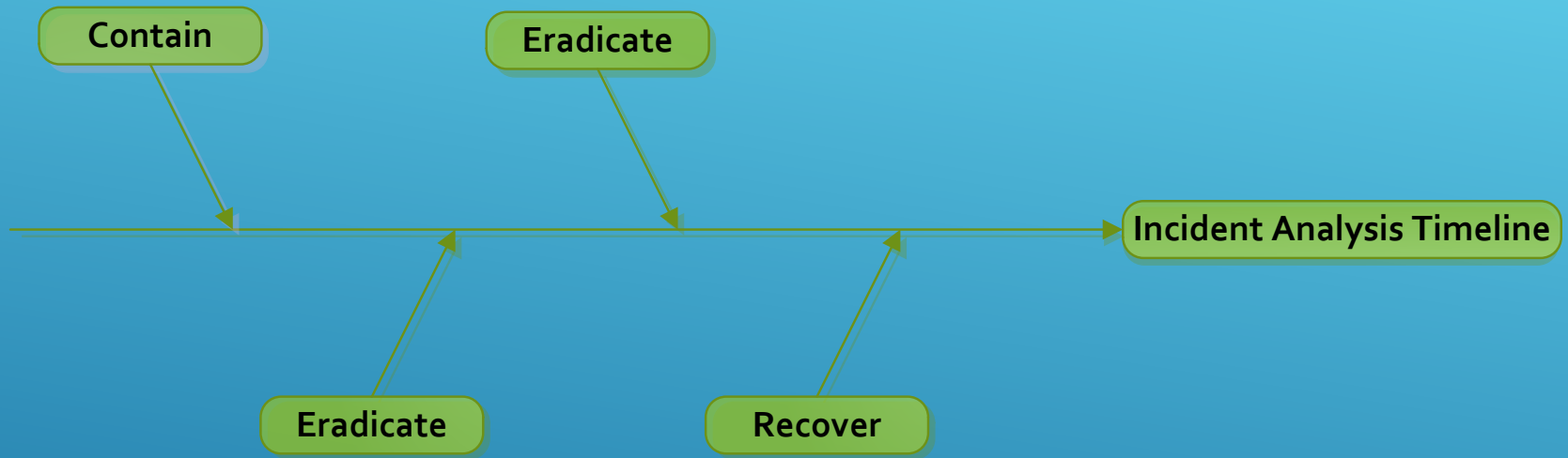
INCIDENT CONTAINMENT, ERADICATION AND RECOVERY

- ▶ **Important to get stakeholder input to the extent possible**
 - ▶ **Prevents other incidents**
 - ▶ **E.g. disconnecting HR systems to finish removing malware**
 - ▶ **May interrupt payroll processing if performed at the wrong time**
- ▶ **Other judgment calls during containment**
 - ▶ **Do you want to sit back and observe hacker behavior?**
 - ▶ **Need to judge potential amount of damage to assets from delayed containment**

**INCIDENT CONTAINMENT,
ERADICATION AND RECOVERY –
CONTD.**

- ▶ **IRT members and administrators have to be careful when pulling plug on hackers**
 - ▶ **Hackers can get destructive when found out**
 - ▶ **Remove all local logging information that may lead to their capture, in an effort to cover their tracks**
 - ▶ **Database administrators may set up traps to totally destroy database and all contained data**
 - ▶ **FBI sting operations against hackers**
 - ▶ **Forcibly and speedily remove individuals from keyboards and other input devices**
 - ▶ **Minimizes possibility that hackers might initiate scripts to destroy assets and evidence**
 - ▶ **E.g. Finale in Kingpin**
 - ▶ **Max Butler example case**

**INCIDENT CONTAINMENT,
ERADICATION AND RECOVERY –
CONTD.**



INCIDENT CONTAINMENT, ERADICATION AND RECOVERY TIMELINE

- ▶ **Prepare for the next incident**
 - ▶ IRT members gather their notes and finalize their documentation
- ▶ **Documentation should contain all individual adverse events involved in the incident**
 - ▶ Together with time stamps and assets involved
 - ▶ As well as
 - ▶ Indicate areas of the organization involved in the accident and resulting breach
 - ▶ How threats were handled individually by each department and together under the coordination of the IRT
 - ▶ Extent to which existing procedures were appropriate to handle the issues
 - ▶ Opportunities for improvement
 - ▶ Extent to which assets were appropriately identified and classified
 - ▶ So that IRT could make quick judgment calls as situation evolved
 - ▶ Extent to which information sharing with stakeholders was done satisfactorily
 - ▶ Opportunities for preemptive detection to avoid similar issues from happening
 - ▶ Technical measures necessary to be taken to avoid similar issues in the future

POST-INCIDENT ANALYSIS

- ▶ **Calamitous incident that causes great destruction**
 - ▶ Has huge repercussion throughout the whole organization
 - ▶ Involves multiple sub-incidents
- ▶ **Disaster Recovery (DR)**
 - ▶ Process adopted by the IT organization in order to bring systems back up and running
 - ▶ **Primary objective**
 - ▶ Keep employees and their families safe
 - ▶ Implementation should avoid hazardous situations
 - ▶ May involve moving operations to a redundant site, recovering services and data
 - ▶ **Extremely complex process**
 - ▶ Usually tackled by individuals with years of experience in the organization

DISASTER

▶ USF example

- ▶ In 2002, hardware failure caused all 30,000 student email accounts to be lost
- ▶ DR plan called for re-creation of all student email accounts
 - ▶ Initially empty
 - ▶ But would allow students to start sending and receiving emails
 - ▶ Subsequently, all mailbox data was extracted from tape and restored to the users' mailboxes
- ▶ Entire DR process took about 3 weeks

DISASTER – CONTD.

- ▶ **DR is a piece of the bigger picture**
 - ▶ **Business Continuity Planning (BCP)**
- ▶ **Business continuity planning**
 - ▶ **Process for maintaining operations under adverse conditions**
 - ▶ **Planners contemplate what would happen in case of a disaster**
 - ▶ **What would be minimally necessary to help the organization continue to operate in case of a disaster**
 - ▶ **USF email example**
 - ▶ **Continuity activities involved questions on how students would turn in assignments**
- ▶ **BCP and DR involve and are often led by entities other than IT**
 - ▶ **HR may require all individuals to stay home in a hurricane level 4 or higher**
 - ▶ **IT may need employees to physically be present to shut down machines**
 - ▶ **Co-ordination between these groups will ensure that appropriate actions are performed**

DISASTER – CONTD.

- ▶ **Business Impact Analysis (BIA)**
 - ▶ An important part of BCP
 - ▶ Identification of services and products that are critical to the organization
- ▶ **BIA is related to asset management**
 - ▶ Essential assets are those that directly support the services and products that result from the BIA
- ▶ **BIA dictates prioritization of the DR procedure**

DISASTER – CONTD.

▶ Preliminary DR checklist

- ▶ Call list
 - ▶ Card-sized list of important phone numbers
- ▶ Plans to inform fellow employees if local phone systems are down
- ▶ Plans to sync backup and recovery at local and remote sites
- ▶ Which data should be restored first?
- ▶ Training for data restoration
 - ▶ Are there instructions published somewhere?
 - ▶ If the expectation is that someone will read a 100-page manual before initiating the restore, the procedure must be simplified
- ▶ Are test restores done regularly?
 - ▶ Tapes and other media go bad, get scratched, and become unreadable
- ▶ Are there means to acquire new hardware to quickly replace the hardware damaged by the disaster?
 - ▶ If cyber insurance is involved, does someone know the details on how to activate it?

DISASTER – CONTD.

- ▶ **In all likelihood, you will not get DR responsibilities in the early part of your career**
 - ▶ **Hence not covered in detail in this book**
 - ▶ **Introduction to familiarize with some basic concepts**
 - ▶ **Enable contribution to the process**

DISASTER – CONTD.

A decorative graphic consisting of several parallel white lines of varying lengths, slanted upwards from left to right, located in the bottom right corner of the slide.

- ▶ **Identify the major components of dealing with an incident**
- ▶ **Understand the incident handling lifecycle**
- ▶ **Prepare a basic policy outlining a methodology for the handling of an incident**
- ▶ **Report on the incident to improve preparation for a similar incident in the future**
- ▶ **The elements of disaster recovery and business continuity planning**

SUMMARY